DMP:SK/AFM/MTK
F.#2016R02228

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
- - - - - - - - - - - - X

UNITED STATES OF AMERICA

- against -

SERGEY DENISOFF,

Defendant.

- - - - - - - - - - - - X

TO BE FILED UNDER SEAL

COMPLAINT AND AFFIDAVIT IN SUPPORT OF APPLICATION FOR ARREST WARRANT

(18 U.S.C. § 1349)

Case No. 20-MJ-066

EASTERN DISTRICT OF NEW YORK, SS:

MARK I. RUBINS, being duly sworn, deposes and states that he is a a Detective with the New York City Police Department ("NYPD") and a Task Force Officer with the Federal Bureau of Investigation ("FBI"), duly appointed according to law and acting as such.

In or about and between September 2014 and December 2016, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant SERGEY DENISOFF, together with others, did knowingly and intentionally conspire to devise a scheme and artifice to defraud online advertising companies and businesses, and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, to wit: electronic communications to computers and servers in the United States and elsewhere, emails and

other online communications, and monetary transfers, contrary to Title 18, United States Code, Section 1343.

(Title 18, United States Code, Section 1349)

The source of your deponent's information and the grounds for his belief are as follows:[1]

1. I am a Detective with the NYPD and have been since 2006. For the past three years I have also been assigned as a Task Force Officer with the FBI Financial Cyber Crimes Task Force ("FCCTF"). My responsibilities on the FCCTF include investigating computer intrusions, sophisticated financial frauds and money laundering, among other offenses. Through my training, education and experience, I have become familiar with (a) the manner in which frauds are committed; (b) the methods used by persons committing fraud to launder the proceeds of their criminal activities; and (c) the efforts of persons involved in such activity to avoid detection by law enforcement.

2. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from: (a) my personal participation in the investigation; (b) my review of the investigative file; and (c) reports made to me by witnesses and other law enforcement officers involved in the investigation.

3. The FBI is conducting an investigation into online advertising fraud by certain individuals and businesses. The government's investigation has uncovered evidence

---

[1] Because the purpose of this Complaint is to set forth only those facts necessary to establish probable cause to arrest, I have not described all the relevant facts and circumstances of which I am aware.

that multiple individuals and companies executed online advertising fraud schemes that victimized individuals and businesses in the United States and elsewhere. Specifically, the evidence obtained in the investigation shows that these individuals and companies used computers that they controlled to create the illusion that a real human internet user was viewing an advertisement on a real internet webpage -- when, in fact, a computer was loading the advertisement on a counterfeit webpage via an automated program -- in order to fraudulently obtain a share of the resulting advertising revenue.

4. The defendant SERGEY DENISOFF operated an advertising network that purported to place ads on real webpages that real human internet users were viewing when, in fact, DENISOFF, together with others, placed ads on dummy webpages that he and others had created and directed automated computers to register views of those ads. Six individuals with whom DENISOFF conspired have been indicted in connection with this scheme in the Eastern District of New York, including Aleksandr Zhukov, Boris Timokhin, Mikhail Andreev, Denis Avdeev, Dmitry Novikov, and Sergey Ovsyannikov (the "Methbot defendants"). See Case No. 18-CR-633 (ERK).

Online Advertising Fraud

5. Based on my knowledge, training and experience, and consultation with experts in cybercrime and online advertising fraud, "advertising fraud" is generally a type of cybercrime in which malicious actors fraudulently obtain money from online advertising companies and businesses. In the subtype of advertising fraud known as an "impression" fraud scheme, internet advertisers are made to believe that advertisements they place are viewed by real human internet users (an occurrence known as an "impression"), when in fact the advertisements are automatically loaded onto computers controlled by the

malicious actors and are not viewed by real human internet users. In the subtype of advertising fraud known as a "click" fraud scheme, internet advertisers are made to believe that advertisements they place are clicked on by real human internet users, when in fact the advertisements are automatically activated by computers controlled by the malicious actors and are not clicked on by real human internet users.

6. In conjunction with fake impressions and fake clicks, malicious actors carrying out an impression fraud or click fraud commonly send out falsified data to fraudulently represent that advertisements are being viewed or clicked on by real human internet users, ultimately resulting in the issuance of payments by advertisers. The malicious actors have business arrangements in place that allow them to claim a portion of those payments. The process of falsifying data to indicate that an advertisement is being viewed or clicked on by a real human internet user in the context of a particular website is known as "domain spoofing," or, more simply, "spoofing."

Overview of The Criminal Scheme

7. By way of an overview, and as further described below, the Methbot defendants operated a purported advertising network called Mediamethane. DENISOFF and others operated a purported advertising network called Plexious. Mediamethane had business arrangements with other advertising networks, such as Plexious, that enabled it to receive payment in return for placing ad tags with publishers on behalf of those advertising networks. Rather than place these ad tags on real publishers' websites, however, Mediamethane maintained a network of computers located at a commercial server farm in Dallas, Texas. The Methbot defendants wrote computer code that caused these computers to simulate the internet activity of human internet users. At the Methbot defendants'

instruction, the computers purported to load webpages belonging to well-known publishers, including publishers in the Eastern District of New York. Mediamethane was paid in return for the purported impressions.

8. In order to disguise the true nature of these automated internet browsers, the Methbot defendants created fraudulent entries in a global register that made it appear that the computers belonged to real internet users, rather than being located in a server facility. The Methbot defendants also programmed their computers to automatically engage in activity (such as mouse movements and scrolling) that would create the impression of control by individual human users.

The Methbot Scheme and the Methbot Defendants

9. On or about December 20, 2016, researchers at a private cybersecurity firm based in New York, New York published a white paper titled "The Methbot Operation," revealing the operation of an online advertising fraud scheme. In the white paper, the cybersecurity firm revealed the IP addresses of computers used to carry out the fraud (the "Malicious IPs"). The cybersecurity firm identified the Malicious IPs based on its monitoring of network traffic related to advertisement impressions on behalf of various advertising clients. It explained that, based on its observations, computers associated with the Malicious IPs transmitted false data to create the impression that a real human internet user was viewing an advertisement on a real internet webpage, when in fact a computer that was not controlled by an individual human was loading the advertisement on a counterfeit webpage. It further explained that the Malicious IPs were associated with false registration data in publicly available IP registration databases. Law enforcement agents reviewed a

sample of the cybersecurity firm's traffic data and confirmed that it was associated with anomalous activity.

10. In or about July 2017, a major U.S. technology company that provides, among other things, advertising services for individuals and businesses informed law enforcement agents that it had corroborated the cybersecurity firm's observations. Specifically, the technology company also monitors traffic data associated with advertisement impressions on behalf of various advertising clients, and noted that the Malicious IPs were associated with fraudulent traffic and bore a common signature.

11. Records obtained from the cybersecurity firm revealed more than 5,000 domains associated with online publishers that the malicious actors had counterfeited, including the domains of thousands of businesses in the United States and multiple businesses in the Eastern District of New York. Records obtained from the technology company revealed that the technology company had reimbursed its clients more than seven million dollars, collectively, for advertising fees that resulted from advertisements that had been fraudulently loaded by computers and not actually viewed by real human internet users. These clients included hundreds of businesses in the United States, including at least one business with offices in the Eastern District of New York.

12. Records obtained from a company that archives IP registration data revealed that many of the Malicious IPs purported to be registered to one or another of six major U.S. internet service providers, including at least one provider with offices in the Eastern District of New York. However, information obtained from the six internet service providers revealed that none of the Malicious IPs registered in their respective names was actually in their possession, custody or control.

13. Law enforcement agents investigated the publicly available registration data for the Malicious IPs and discovered information linking the Malicious IPs to Zhukov and his co-conspirators.

14. More than 1,400 Malicious IPs were registered to an email address identified herein as the "Registration Email Account." The Registration Email Account communicated with accounts that were controlled by Zhukov.

15. Zhukov sent emails in which he identified himself as the CEO of a purported advertising network called Mediamethane. Law enforcement agents reviewed communications indicating that both Zhukov and Timokhin used email accounts with the domain mediamethane.com. The registrant of Zhukov's account at mediamethane.com listed an account controlled by Zhukov as a recovery email address.

16. In reviewing the returns from the search warrants, law enforcement agents observed invoices and communications from a server provider in Dallas, Texas reflecting that, beginning in mid-2015, Zhukov and Timokhin rented hundreds of servers from the server provider.

17. Relatedly, law enforcement agents observed records and communications reflecting that Zhukov and his co-conspirators rented hundreds of thousands of IP addresses from various IP address leasing companies and then registered those IP addresses with false information. For example, on May 13, 2016, co-conspirator Denis Avdeev communicated with an employee of an IP leasing company and instructed the employee to make certain changes to the location and usage information associated with the leased IP addresses. Specifically, Avdeev directed that the IP leasing company change the "Usage type" for the leased IP addresses from "commercial" or "datacenter" to "ISP"

(internet service provider); ascribe a more diverse set of cities and states to the leased IP addresses; and reduce the number of leased IP addresses associated with certain small cities (Avdeev commented that "200,000 IP in the city [of] Wilmington with a population [of] 71,525 [is] overly [sic]").

18. Based on my knowledge, training and experience, the foregoing measures were intended to disguise the rented servers to make them appear as if they were legitimate computers from various locations across the United States and elsewhere, rather than a set of servers located in a single datacenter, in order to create the illusion that real human internet users were at the controls of the computers.

19. Law enforcement agents also observed a note related to IP address registration in the cloud storage account associated with Zhukov's email account. In the note, which is dated September 18, 2015, Zhukov listed numerous false corporate names that mimicked the names of various major U.S. internet service providers. The list included the false names associated with many of the Malicious IPs in publicly available IP registration data (supra ¶ 16).

20. During their review of the returns from search warrants on Zhukov's email account and Timokhin's email account, law enforcement agents observed a series of communications between and among the Methbot defendants using a specific online collaboration tool designed for software project management (the "Collaboration Software") that allows messages to be posted within a secure shared space. The Collaboration Software caused each message to be automatically emailed to Zhukov's email account and Timokhin's email account from a separate email account. The communications included discussions related to the development of software code that would direct servers to simulate human

beings viewing online advertisements. For example, on October 25, 2014, co-conspirator Mikhail Andreev circulated programming code designed to ensure that signals coming from the computers had the correct "'browser' parameters." Based on my knowledge, training and experience, Andrrev's use of quotation marks around the word "browser" indicates that the conspirators custom-designed an automatic web browser so that it could mimic signals sent by typical internet browsers that a real human would operate. Later that same day, Andreev posted a message stating that he had implemented the code and speculated that it was "possible to click ten times per hour."

21. On October 31, 2014, Andreev posted a message using the collaboration software that stated, "Dmitry Novikov, write in detail how it should be proceeding? 'This many clicks per hour' or 'This many clicks per day.'" On December 28, 2014, Zhukov posted a message complaining that the computers were clicking too rapidly, stating: "Mikhail Andreev set . . . 10 clicks per day per IP. However, within an hour it already downloaded 300 clicks. It has to be a bug. It should be about 50-60 clicks per hour total."

22. On October 28, 2014, co-conspirator Dmitry Novikov posted a message using the collaboration software titled, "Make mouse move and scroll more meaningful." In the message, Novikov directed Timokhin to carry out "research about how to make 'mouse moves and scroll more realistic/meaningful.'" Similarly, on June 25, 2015, Zhukov sent a "to-do" list to Timokhin directing him to address a "lack of mouse move." Based on my knowledge, training and experience, the foregoing messages reveal an effort to remotely induce mouse movements in computers in order to create the illusion that real human internet

users were at the controls of the computers for the purpose of misleading security software deployed by advertisers.

23. In Zhukov's June 25, 2015 to-do list, Zhukov also instructed Timokhin "to add authorization for Facebook [] users. There is Google, twitter too; [but] no FB (There should be approximately 40% of them.)" Based on my knowledge, training and experience, the foregoing comment reveals an effort to make computers appear to be signed into Facebook in order to further create the illusion that real human internet users were at the controls of the computers.

24. Other messages posted by the conspirators using the Collaboration Software dealt specifically with nonhuman viewing of video advertisements. For example, on October 28, 2014, Novikov posted a message titled "Emulating 'video watch,'" in which he cautioned, "The videos need to be clicked on and watched for 60-90 seconds." Based on my knowledge, training and experience, the foregoing message reveals an effort to ensure that a sufficient portion of each advertisement was watched to ensure payment by advertisers. On December 1, 2014, Andreev circulated programming code designed to cause computers to automatically play and pause an online video player and wrote, "Basically this is how it is possible to generate the events." Based on my knowledge, training and experience, the foregoing message reveals efforts to start and stop a video, rather than playing it all the way through or not at all, in order to further create the illusion that real human internet users were at the controls of the computers.

25. The conspirators explicitly discussed their efforts to evade security software deployed by advertisers and SSPs to detect nonhuman browsing. Such software is typically sold and operated by third-party cybersecurity vendors. For example, in a note

dated August 4, 2015, found within the cloud storage account associated with Zhukov's email account, Zhukov referred to two specific U.S. cybersecurity firms and wrote that he intended to "check [] out [their] filter for the possibility of fucking them over a la," followed by the name of a third firm. Based on my knowledge, training and experience, the note indicates that Zhukov was making efforts to understand and evade cybersecurity firms' detection software (or "filters").

26. Similarly, on October 12, 2016, Zhukov directed Timokhin to "turn[] off the block" on a certain cybersecurity firm. Based on my knowledge, training and experience, the foregoing message reveals that the conspirators had programmed their system not to load advertisements that deployed fraud detection software supplied by the referenced firm. Finally, on October 16, 2016, after discovering that his online advertising impressions did not register as fraudulent with a certain cybersecurity firm, Zhukov wrote a celebratory email to Timokhin stating that their scheme "[was] magnificent."

27. The defendants made a selling point of Mediamethane's ability to provide advertising traffic that did not trigger fraud detection software and registered as coming from United States computers. For example, on October 12, 2016, Zhukov sent an email to a potential business partner in which he offered "100% USA traffic" that could pass through "filters" from various U.S. cybersecurity firms that monitor internet traffic for fraudulent activity and amounted to "20-50 millions [sic] impressions daily."

The Defendant's Membership in the Methbot Conspiracy

28. During their review of the returns from search warrants on Zhukov's email account, law enforcement agents observed email communications between Zhukov and the email address sergey@plexious.com ("Denisoff Email Account 1").

29. During the investigation, law enforcement agents gathered information that appears to confirm that SERGEY DENISOFF used Denisoff Email Account 1. For example, the user of Denisoff Email Account 1 sent emails signed "Sergey Denisoff" and that identified him as the "Director of Business Development" for a business called "Plexious." In addition, records obtained from the service provider for Denisoff Email Account 1 revealed that the account was registered to "Sergey Denisoff" and had been accessed from a location in Woodland Hills, California. Finally, when law enforcement agents interviewed DENISOFF at his residence in Woodland Hills, California, as further described below, DENISOFF admitted to having used Denisoff Email Account 1.

30. Law enforcement agents observed email communications in which DENISOFF assisted Zhukov with carrying out the Methbot scheme. For example, on November 20, 2015, DENISOFF sent Zhukov an email with the subject line "new sites" listing dozens of domains. On November 24, 2015, DENISOFF sent Zhukov another email, this one with the subject line "more sites," again listing dozens of domains. Zhukov forwarded both emails to Timokhin. Records obtained from the Internet Archive[2] revealed that many of these domains hosted dummy webpages -- that is, webpages that appeared to belong to popular internet sites but were actually mere placeholders for placing ads in furtherance of the fraudulent scheme. For example: some of the webpages contained the exact same articles and other content that was found on some of the other webpages; some of the webpages contained the Latin text that appears by default in webpage editors (which begin with the words "lorem ipsum"); most of the webpages lacked indicia of having been

---

[2] The Internet Archive is an online repository of internet webpages as they appeared at certain points in time.

visited by real human internet users, in that there were no "likes" or other comments on articles; and at least one of the webpages contained only articles written by a user with the moniker "plex11186." Based on my knowledge, training, and experience, and the facts of this investigation, I understand the emails from DENISOFF to Zhukov listing domains as evidence of DENISOFF supplying the Methbot defendants with fraudulent domains for placing ads in furtherance of the fraudulent scheme.

31. On October 19, 2019, law enforcement agents conducted a voluntary interview of DENISOFF at his residence in Woodland Hills, California.[3] At the outset of the interview, DENISOFF acknowledged that he was speaking to the interviewers voluntarily and could direct them to leave at any point. During the interview, DENISOFF explained that in approximately the years 2011-2012, he and a former friend from college learned how the online advertising ecosystem worked and launched an ad network that they named Plexious. Plexious worked with other ad networks to source and resell ad traffic. Specifically, the main business of Plexious was to buy "bullshit" popup traffic from suppliers and resell it to buyers in demand of that "bullshit" traffic. Plexious initially supplied traffic pursuant to the pay-per-click traffic model (where traffic is monetized by users clicking on links) and eventually transitioned (along with the rest of the industry) to the video and display advertisement traffic model.

32. DENISOFF explained that fraudulent traffic could come from computers located in a commercial datacenter, among other things. He further explained that Plexious hired various cybersecurity firms that deployed fraud detection software and

---

[3] All statements from the interview described herein are in sum and substance and in part, unless otherwise indicated.

observed that many of them did not flag fraudulent traffic that was originating from computers located in a commercial datacenter. DENISOFF added that various ad networks also engaged in fraudulent practices like using fabricated webpages and IP address information -- and described in detail how such fabrication works -- but stated that neither he nor Plexious had engaged in any such fraudulent practices and, furthermore, he cut off certain suppliers who had.

33. When asked about the emails he sent Zhukov listing domains (see supra ¶ 41), DENISOFF stated that: he and his business partner registered about a hundred domains, which he called "Test Pages"; he did business with ad networks who supplied traffic to those Test Pages; and sometimes he placed actual ads on those Test Pages and received money for the resulting impressions. DENISOFF noted that Plexious partnered with Zhukov and other supply-side partners for the supply of ad traffic. DENISOFF claimed that advertising agencies and ad networks that paid DENISOFF for ad traffic should have known that most people would not visit such "bullshit" domains to search for information.

34. DENISOFF stated that Plexious earned approximately $10-12 million in revenue between the years 2012 and 2016, most of which came from video traffic. He further stated that he left the ad industry in approximately the years 2015-2016.

35. Records obtained from Microsoft revealed that, later in the evening on October 19, 2019, DENISOFF accessed Denisoff Email Account 1 from an IP address associated with Woodland Hills, California -- the location of the residence where agents had interviewed DENISOFF earlier that day.

36. During the investigation, law enforcement agents observed additional communications between DENISOFF and Zhukov. On November 6, 2018, foreign law enforcement authorities in Bulgaria arrested Zhukov, searched his apartment, and seized his computer. Foreign authorities subsequently extradited Zhukov to the United States and provided U.S. law enforcement authorities with Zhukov's computer and other items seized from his apartment in Bulgaria. A review of Zhukov's computer revealed multiple communications over the online messaging platform Skype between Zhukov and an individual with the username "sergey-plexious." Information gathered during the investigation appears to confirm that DENISOFF used the Skype username "sergey-plexious." Specificlly, records obtained from Microsoft revealed that the Skype username "sergey-plexious" is an alias of Denisoff Email Account 1.

37. DENISOFF and Zhukov communicated over Skype in furtherance of the Methbot scheme. For example, on August 27, 2015, Zhukov noted that they were having problems with 50 of their servers ("50 servers still messing up our entire picture"), noted that "[i]n order to activate all servers we need to finish tests . . .," and asked DENISOFF, "Could you test our traffic?" DENISOFF responded, "It has gotten much better," and approximately two hours later DENISOFF reported back, "Yes, the traffic that you are routing to [his domain] for the past couple of hours is working." Zhukov responded, "awesome." Based on my knowledge, training, and experience, and the facts of this investigation, I understand the foregoing as Zhukov obtaining DENISOFF's assistance to test whether the servers that Zhukov rented from the commercial datacenter and programmed to commit ad fraud were successfully transmitting fraudulent ad traffic to DENISOFF's domain without being flagged by cybersecurity firms' fraud detection software.

38. Later in the conversation, DENISOFF explained to Zhukov which cybersecurity firms' software needed to be circumvented, stating that a certain ad platform did "not check for quality through" one U.S. cybersecurity firm and instead another U.S. cybersecurity firm was "more important." DENISOFF further advised Zhukov on the types of information that the cybersecurity firms detected and shared in their reports. DENISOFF further advised Zhukov on how traffic statistics should appear to mimic real human ad traffic. For example, DENISOFF provided Zhukov with sample percentages of individuals that watch a video ad part of the way versus all the way, and how such reporting should look, so that Zhukov could structure his fraudulent views to mimic real human internet users' behavior.

39. Midway through the foregoing conversation, DENISOFF told Zhukov, "By the way, lets switch to jabber before they put me in jail." DENISOFF explained later in the conversation that "we need something without logs and access from the American law enforcement." Based on my knowledge, training, and experience, Jabber is an online messaging platform that is decentralized and run by users from their own servers; therefore, there is often no central company or service that can provide the contents of Jabber communications in response to legal process. DENISOFF provided Zhukov with his Jabber username as "primusad@jabber.ru";[4] Zhukov noted that he had Jabber on his computer.

40. A review of Zhukov's computer revealed multiple communications over Jabber by Zhukov, DENISOFF, and other during the course of the Methbot scheme.

---

[4] It should be noted that when law enforcement agents interviewed DENISOFF, California, DENISOFF stated that his business partner was possibly the individual using the "primusad@jabber.ru" Jabber username.

During the communications, DENISOFF discussed the routing of Zhukov's fraudulent ad traffic to his domains, whether the ad traffic was being flagged by cybersecurity firms, and the amount and nature of payments sent and received in connection with the scheme.

WHEREFORE, your deponent respectfully requests that an arrest warrant be issued for the defendant SERGEY DENISOFF, so that he be dealt with according to law.

MARK I. RUBINS
Detective, New York City Police Department

Sworn to before me this
17th day of January, 2020

THE HONORABLE RAMON E. REYES, JR.
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK